AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Original) A method of generating a password for use by an end-user device (UE) to access a remote server, comprising:

sending a request for access from the UE to the remote server;

creating a temporary identity for the UE;

sending to an authentication node in the UE's home network details of the request for access;

at the authentication node or the remote server, generating a Hypertext Transfer Protocol (HTTP) Digest challenge using an algorithm capable of generating end-user passwords, including details of the temporary identity of the UE ;

at the UE, generating a password based on the HTTP Digest challenge, said password being associated with the identity of the remote server and the identity of the UE ; and

storing the password and the temporary identity of the UE at the UE.

2. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 1, wherein the algorithm capable of generating end-user passwords is HTTP Digest Authentication and Key Agreement (AKA).

3. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 1 ~~or 2~~, further comprising sending the identity of the remote server to the authentication node, wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server, and wherein the identity of the remote server is stored at the UE.

4. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 1, ~~2 or 3~~, wherein the temporary identity of the UE is created at the remote server.

5. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 1 ~~any preceding claim~~, wherein the step of sending details of the request for access to the authentication node includes redirecting the request for access to the authentication node.

6. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 5, wherein the HTTP Digest challenge is generated at the authentication node and sent from the authentication node directly to the UE.

7. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 5 ~~or 6~~, wherein the password is stored at the authentication node.

8. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 5, ~~6 or 7,~~ further comprising authenticating the UE at the authentication node and redirecting the request for access from the authentication node ~~back~~ to the remote server after the password has been generated.

9. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 1 ~~any of claims 1 to 4~~, wherein the step of sending details of the request for access to the authentication node includes the remote server contacting the authentication node directly.

10. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 9, wherein the HTTP Digest challenge is generated at the authentication node and sent from the authentication node to the remote server.

11. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 9, wherein the HTTP Digest challenge is generated at the remote server.

12. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 10 ~~or 11~~, further comprising sending the HTTP digest challenge from the remote server to the UE.

13. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 11, further comprising including a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server and authenticating the UE at the remote server.

14. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 9 ~~any of claims 9 to12~~, further comprising authenticating the UE at the authentication node and returning an authentication result to the remote server.

15. (Currently Amended) A method of accessing a remote server from an end-user device (UE), the method comprising:

generating and storing a password; ~~using a method as claimed in any of the preceding claims~~;

sending a request for access from the UE to the remote server ;

at the remote server, generating a Hypertext Transfer Protocol (HTTP) Digest challenge including details of the identity of the remote server and sending the challenge to the UE; and

at the UE, sending an authentication response including the temporary identity of the UE and a proof of possession of the password to the remote server.

16. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 15, further comprising sending an authentication request from the remote server to the authentication node, sending the password from the authentication node to the remote server, and authenticating the UE at the remote server.

17. (Currently Amended) The [[A]] method ~~as claimed~~ in claim 15, further comprising sending an authentication request from the remote server to the

authentication node, authenticating the UE at the authentication node, and sending confirmation of authentication from the authentication node to the remote server.

18. (New) The method of claim 15, wherein the step of generating and storing a password further comprises:

creating a temporary identity for the UE;

sending to an authentication node in the UE's home network details of the request for access;

at the authentication node, generating a Hypertext Transfer Protocol (HTTP) Digest challenge using an algorithm capable of generating end-user passwords including details of the temporary identity of the UE;

at the UE, generating a password based on the HTTP Digest challenge, said password being associated with the identity of the remote server and the identity of the UE ; and

storing the password and the temporary identity of the UE at the UE.

19. (New) The method in claim 18, wherein the algorithm capable of generating end-user passwords is HTTP Digest Authentication and Key Agreement (AKA).

20. (New) The method in claim 18, further comprising sending the identity of the remote server to the authentication node, wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server, and wherein the identity of the remote server is stored at the UE.

22. (New) The method in claim 18, wherein the temporary identity of the UE is created at the remote server.

23. (New) The method in claim 18, wherein the step of sending details of the request for access to the authentication node includes redirecting the request for access to the authentication node.

24. (New) The method in claim 23, wherein the HTTP Digest challenge is generated at the authentication node and sent from the authentication node directly to the UE.

25. (New) The method in claim 23, wherein the password is stored at the authentication node.

26. (New) The method in claim 23, further comprising authenticating the UE at the authentication node and redirecting the request for access from the authentication node to the remote server after the password has been generated.

27. (New) The method in claim 18, wherein the step of sending details of the request for access to the authentication node includes the remote server contacting the authentication node directly.

28. (New) The method in claim 27, wherein the HTTP Digest challenge is generated at the authentication node and sent from the authentication node to the remote server.

29. (New) The method in claim 27, wherein the HTTP Digest challenge is generated at the remote server.

30. (New) The method in claim 28, further comprising sending the HTTP digest challenge from the remote server to the UE.

31. (New) The method in claim 29, further comprising including a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server and authenticating the UE at the remote server.

32. (New) The method in claim 28, further comprising authenticating the UE at the authentication node and returning an authentication result to the remote server.